PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :
G06F 11/16, G05B 9/03, 19/05, G06F 11/277

A1

(11) Internationale Veröffentlichungsnummer: **WO 98/38577**

(43) Internationales Veröffentlichungsdatum: 3. September 1998 (03.09.98)

(21) Internationales Aktenzeichen: PCT/EP98/00827

(22) Internationales Anmeldedatum: 13. Februar 1998 (13.02.98)

(30) Prioritätsdaten:
97103151.3 26. Februar 1997 (26.02.97) EP
(34) Länder für die die regionale oder internationale Anmeldung eingereicht worden ist: DE usw.

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D–80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: BARTHEL, Herbert [DE/DE]; Am Hasengarten 6A, D–91074 Herzogenaurach (DE). VON KROSIGK, Hartmut [DE/DE]; Platanenweg 3, D–91058 Erlangen (DE).

(81) Bestimmungsstaaten: CN, JP, KR, SG, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

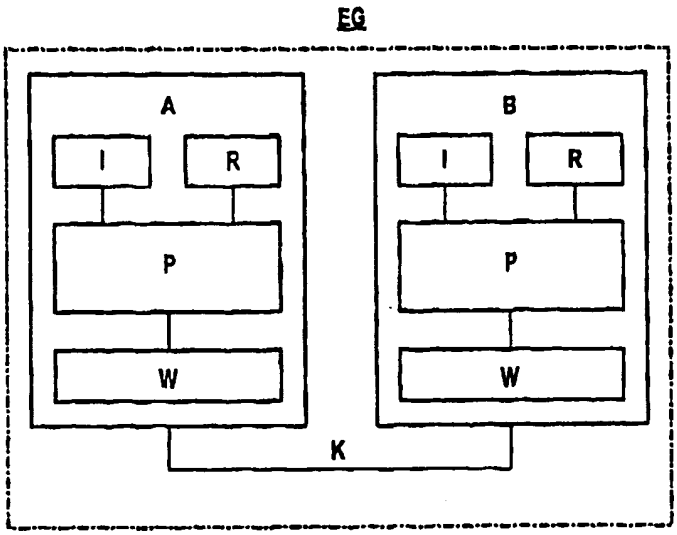
Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: REDUNDANT ELECTRONIC DEVICE WITH CERTIFIED AND NON–CERTIFIED CHANNELS

(54) Bezeichnung: REDUNDANT AUFGEBAUTES ELEKTRONISCHES GERÄT MIT ZERTIFIZIERTEN UND NICHT ZERTIFIZIERTEN KANÄLEN

(57) Abstract

The invention relates to a homogeneously and redundantly built electronic device (EG) with at least two channels, especially a two–channel, homogeneously and redundantly built programmable central unit of a controller with at least one certified channel (A) and at least one non–certified channel (B). Said certified channel (A) is a channel (A) which is sufficiently free of systematic faults whilst in the non–certified channel (B), components can be used which have not been explicitly proven to be sufficiently free of systematic faults.



(57) Zusammenfassung

Zumindest zweikanalig homogen redundant aufgebautes elektronisches Gerät (EG), insbesondere zweikanalig homogen redundant aufgebaute Zentraleinheit einer speicherprogrammierbaren Steuerung, mit zumindest einem zertifizierten Kanal (A) und zumindest einem nicht zertifizierten Kanal (B), wobei der zertifizierte Kanal (A) ein von systematischen Fehlern ausreichend freier Kanal (A) ist, und wobei im nicht zertifizierten Kanal (B) Komponenten einsetzbar sind, deren ausreichende Freiheit von systematischen Fehlern nicht explizit nachgewiesen ist.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Beschreibung

Redundant aufgebautes elektronisches Gerät mit zertifizierten und nicht zertifizierten Kanälen

Die vorliegende Erfindung betrifft ein zumindest zweikanalig aufgebautes elektronisches Gerät, insbesondere eine zweikanalig aufgebaute programmierbare Logik, wobei diese programmierbare Logik beispielsweise die Zentraleinheit einer speicherprogrammierbaren Steuerung sein kann.

Für sicherheitsrelevante Aufgaben werden elektronische Geräte benötigt, die in hohem Maße funktionssicher sind, wobei der Ausdruck „funktionssicher" in Anlehnung an den Ausdruck „functional safety" des internaltionalen Schriftstücks Draft-IEC 1508 gewählt wurde.

Funktionssichere elektronische Geräte zeichnen sich dadurch aus, daß für sie spezielle Maßnahmen vorgesehen sind, um Fehler und Ausfälle zu vermeiden, zu erkennen und zu beherrschen.

Eine gebräuchliche Methode zum Vermeiden, Erkennen und Beherrschen von Fehlern und Ausfällen ist die mehrkanalige, redundante Ausführung elektronischer Geräte - in den jeweiligen Kanälen werden gleiche Operationen parallel ausgeführt. Durch Vergleich der Ergebnisse bzw. Ausgangswerte wird erkannt, ob in einem der Kanäle ein Fehler aufgetreten ist.

Eine bestimmte Gruppe von Fehlern, die für die Gewährleistung eines funktionssicheren Betriebs von besonderer Relevanz sind, sind die sogenannten systematischen Fehler einer Baugruppe, eines Bauteils oder einer Komponente eines Kanals. Derartige Fehler können z.B. durch die logische Struktur,

d.h. die Verschaltung der einzelnen Komponenten und Baugruppen untereinander, oder deren physikalischen Eigenschaften, die durch den jeweils angewandten Herstellungsprozeß bedingt sind, begründet sein. Die für die vorgesehene Anwendung ausreichende Freiheit von systematischen Fehlern wird durch umfangreiche Zertifizierungsmaßnahmen nachgewiesen.

Bei der heutigen schnellen Entwicklung der Halbleitertechnologie werden die Herstellungsprozesse bereits nach kurzer Zeit gewechselt. Dies hat zur Folge, daß für die betreffenden Komponenten und Baugruppen ihre Freiheit von systematischen Fehlern immer wieder neu nachgewiesen werden muß, denn der Betrieb derartiger Komponenten und Baugruppen in einem als funktionssicher eingestuften System ist nur nach umfangreichen Zertifizierungsmaßnahmen zulässig.

Der schnelle Innovationszyklus im Bereich der Halbleiter hat zur Folge, daß diese Zertifizierung z.B. mit jeder neuen Mikroprozessorgeneration oder jeder neuen Speicherbausteingeneration neu durchgeführt werden muß, wobei die für den Zertifizierungsprozeß aufgrund der für die zu erbringenden Tests und/oder der für den Nachweis der Betriebsbewährtheit zu veranschlagenden Zeit dazu führt, daß neuartige Bauteile erst mit erheblicher Verzögerung für sicherheitsrelevante Anwendungen eingesetzt werden können.

Die Aufgabe der vorliegenden Erfindung besteht folglich darin, ein elektronisches Gerät anzugeben, mit dem es möglich ist, in sicherheitsrelevanten Systemen mit homogen redundanten Kanälen Baugruppen, Bauteile oder Komponente zu betreiben, für welche die ausreichende Freiheit von systematischen Fehlern noch nicht nachgewiesen wurde.

Die Aufgabe wird für das elektronische Gerät dadurch gelöst, daß das zumindest zweikanalig homogen redundant aufgebaute

elektronische Gerät, das insbesondere eine zweikanalig homogen redundant aufgebaute programmierbare Logik sein kann, zumindest einen zertifizierten Kanal und zumindest einen nicht zertifizierten Kanal aufweist, wobei der zertifizierte Kanal ein von systematischen Fehlern ausreichend freier Kanal ist.

Als von systematischen Fehlern ausreichend freier Kanal wird in diesem Zusammenhang ein Kanal verstanden, dessen Versagenswahrscheinlichkeit über einen bestimmten Zeitraum eine bestimmte, durch die jeweilige Anwendung beeinflußte Schwelle, die z.B. eine Schwelle nach dem internationalen Schriftstück Draft-IEC 1508 sein kann, nicht überschreitet.

Wenn für jeden Kanal ein abfragbares Kennzeichen, z.B. eine spezielle Speicherzelle oder ein mechanischer oder elektronischer Schalter vorgesehen ist, wobei beim Abfragen des Kennzeichens für einen zertifizierten Kanal eine erste Kennung bzw. für einen nicht zertifizierten Kanal eine zweite Kennung ermittelbar ist und das elektronische Gerät seinen Betrieb nur dann aufnimmt, wenn bei der Abfrage der Kennung der einzelnen Kanäle zumindest einmal die erste Kennung auftritt, so ist damit für das elektronische Gerät ein Selbsttest realisiert, der gewährleistet, daß das elektronische Gerät seinen Betrieb nur dann aufnimmt, wenn sichergestellt ist, daß mindestens einer der Kanäle des mindestens zweikanalig aufgebauten elektronischen Gerätes ein von systematischen Fehlern ausreichend freier, d.h. zertifizierter Kanal ist.

Wenn die Abfrage der Kennung der einzelnen Kanäle sequentiell erfolgt, ist eindeutig ermittelbar, welcher der Kanäle ein von systematischen Fehlern ausreichend freier, d.h. zertifizierter Kanal ist und welcher der Kanäle ein von systematischen Fehlern nicht ausreichend freier, d.h. nicht zertifizierter Kanal ist.

Wenn die Kennung des nicht zertifizierten Kanals beim Betrieb des elektronischen Gerätes nach einer vorgebbaren, von erkannten Fehlern freien Zeitspanne von der zweiten Kennung, die den Kanal als nicht zertifiziert charakterisiert, auf die erste Kennung, die den Kanal als zertifiziert charakterisiert, wechselbar ist, ist nach ausreichender Betriebsdauer und Bewertung des Betriebsverhaltens des bisher nicht zertifizierten Kanals dieser Kanal selbst als Referenzkanal einsetzbar, so daß mit dem elektronischen Gerät z.B. Bauteile, Komponenten oder Baugruppen der übernächsten Generation, die natürlich noch nicht zertifiziert sind, eingesetzt werden können, ohne vorher deren Fehlerfreiheit nachweisen zu müssen.

Weitere Vorteile und erfinderische Einzelheiten ergeben sich aus der nachfolgenden Beschreibung eines Ausführungsbeispiels anhand der Zeichnung und in Verbindung mit den Unteransprüchen. Im einzelnen zeigt:

FIG 1 ein Blockschaltbild einer zweikanalig homogen redundant aufgebauten Zentraleinheit einer speicherprogrammierbaren Steuerung.

Gemäß FIG 1 ist das elektronische Gerät EG eine zweikanalig homogen redundant aufgebaute Zentraleinheit einer speicherprogrammierbaren Steuerung. Homogene Redundanz bezeichnet hier die Tatsache, daß die einzelnen Kanäle symmetrisch mit zumindest funktionsgleichen Bauteilen, Komponenten oder Baugruppen aufgebaut sind.

Beim Ausführungsbeispiel gemäß FIG 1 weist der Kanal A einen Mikroprozessor P, einen Programmspeicher I und einen Datenspeicher R auf. Der Betrieb des Mikroprozessors P wird mittels einer Überwachungseinheit W, eines sogenannten Watchdogs Wüberwacht. Der Kanal B ist homogen redundant zum Kanal A

aufgebaut, was insbesondere anhand der gleichen Komponenten P, I, R, die jeweils auch mit gleichen Bezugszeichen versehen sind, deutlich wird.

Kanal A muß aus den Komponenten P, I, R, W aufgebaut sein, für die die Freiheit von systematischen Fehlern ausreichend nachgewiesen ist, mithin die jeweiligen Komponenten, Bauteile und Baugruppen also zertifiziert sind. Damit stellt sich Kanal A insgesamt als von systematischen Fehlern ausreichend freier Kanal A dar.

In Kanal B werden eine oder mehrere Komponenten P, I, R, W in Versionen eingesetzt, die in irgendeiner Weise verändert wurden, z.B. aufgrund eines neuen oder geänderten Fertigungsprozesses, und für die die Freiheit von systematischen Fehlern noch nicht ausreichend nachgewiesen ist.

Werden in den betreffenden Bauteilen, Komponenten oder Baugruppen von Kanal B eventuell vorhandene systematische Fehler wirksam, werden diese durch Ergebnisvergleich mit Kanal A, der über die Kopplung K, die zwischen den Kanälen A und B besteht, durchführbar ist, erkannt und können somit beherrscht werden.

Damit ist es möglich, ohne Verschlechterung der Sicherheitseigenschaften in einem Kanal A, B des redundanten elektronischen Gerätes EG Bauteile, Komponenten oder Baugruppen zu verwenden, deren Fehlerfreiheit noch nicht ausreichend nachgewiesen ist, die mithin noch nicht zertifiziert sind.

Mit Hilfe des Ergebnisvergleichs werden systematische Fehler, die z.B. durch die physikalischen Eigenschaften der jeweiligen elektronischen Bauteilen, Komponenten oder Baugruppen oder durch einen veränderten Fertigungs- oder Montageprozeß bedingt sind, erkannt.

Das erfindungsgemäße elektronische Gerät EG erlaubt es dem Anbieter eines derartigen Gerätes unmittelbar auf die Innovationszyklen z.B. der Halbleiterindustrie zu reagieren und auch in funktionssicheren Systemen stets Bauteile, Komponenten oder Baugruppen anzubieten, die dem aktuellen Stand der Entwicklung entsprechen, auch wenn für diese Bauteile deren ausreichende Freiheit von systematischen Fehlern bisher mit einer Zertifizierung noch nicht explizit nachgewiesen ist.

In diesem Zusammenhang muß es als besonders vorteilhaft angesehen werden, daß mit dem erfindungsgemäßen Verfahren bzw. dem erfindungsgemäßen elektronischen Gerät EG diese Zertifizierung implizit zu erreichen ist.

Zu diesem Zweck ist es vorgesehen, daß für jeden Kanal A,B des elektronischen Gerätes EG eine Kennung verwaltet wird, die darüber Aufschluß gibt, ob der jeweilige Kanal A, B als von systematischen Fehlern ausreichend frei angesehen werden kann. Nach einer bestimmten, insbesondere vom Benutzer frei wählbaren Zeitspanne, bei der im Betrieb des elektronischen Gerätes EG im bisher nicht zertifizierten Kanal A, B kein systematischer Fehler erkannt wurde, ist diese Kennung von „nicht zertifiziert" auf „zertifiziert" umschaltbar, so daß auch der bisher explizit nicht zertifizierte Kanal, dessen Freiheit von systematischen Fehlern im konkreten Betrieb ausreichend nachgewiesen ist, wie ein explizit zertifizierter Kanal eingesetzt werden kann.

Dies ermöglicht es insbesondere in einem elektronischen Gerät EG zusmmen mit diesem nunmehr „online-zertifizierten Kanal" in einem weiteren, redundanten Kanal A, B auch Bauteile, Baugruppen oder Komponenten der übernächsten Generation von Halbleiterbauelementen einzusetzen, und sodann entsprechend dem oben beschriebenenen Vorgang auch für diese Komponenten

nach Möglichkeit deren ausreichende Freiheit von systematischen Fehlern nachzuweisen.

Damit ermöglicht der Einsatz des erfindungsgemäßen elektronischen Gerätes EG bzw. die Anwendung des erfindungsgemäßen Verfahrens jederzeit die Verwendung der neuesten Bauteile, Baugruppen oder Komponenten, die ansonsten erst nach einem zeitaufwendigen Zertifizierungsprozeß für die Anwendung in sicherheitsrelevanten Systemen freigegeben werden.

Patentansprüche

1. Zumindest zweikanalig homogen redundant aufgebautes elektronisches Gerät (EG), insbesondere zweikanalig homogen redundant aufgebaute programmierbare Logik, wobei das elektronische Gerät (EG) zumindest einen zertifizierten Kanal (A) und zumindest einen nicht zertifizierten Kanal (B) aufweist, wobei der zertifizierte Kanal (A) ein von systematischen Fehlern ausreichend freier Kanal ist.

2. Elektronisches Gerät nach Anspruch 1, dadurch gekennzeichnet, daß für jeden Kanal (A, B) ein abfragbares Kennzeichen vorgesehen ist, wobei beim Abfragen des Kennzeichens für einen zertifizierten Kanal (A) eine erste Kennung (T) bzw. für einen nicht zertifizierten Kanal (B) eine zweite Kennung (F) ermittelbar ist, wobei das elektronische Gerät (EG) seinen Betrieb nur dann aufnimmt, wenn bei der Abfrage der Kennung der einzelnen Kanäle (A, B) zumindest einmal die erste Kennung (T) vorliegt.

3. Elektronisches Gerät nach Anspruch 2, dadurch gekennzeichnet, daß die Abfrage der Kennung der einzelnen Kanäle (A, B) sequentiell erfolgt.

4. Elektronisches Gerät nach Anspruch 2 oder 3, dadurch gekennzeichnet, daß die Kennung des nicht zertifizierten Kanals (B) nach einer vorggebbaren, von erkannten Fehlern freien Zeitspanne von der zweiten Kennung (F) auf die erste Kennung (T) wechselbar ist.

5. Verfahren zum Betreiben eines zumindest zweikanalig homogen redundant aufgebauten elektronischen Gerätes (EG), insbesondere einer zweikanalig homogen redundant aufge-

bauten programmierbaren Logik, wobei das elektronische Gerät (EG) zumindest einen zertifizierten Kanal (A) und zumindest einen nicht zertifizierten Kanal (B) aufweist, wobei der zertifizierte Kanal (A) ein von systematischen Fehlern ausreichend freier Kanal ist.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß für jeden Kanal (A, B) ein abfragbares Kennzeichen vorgesehen ist, wobei beim Abfragen des Kennzeichens für einen zertifizierten Kanal (A) eine erste Kennung (T) bzw. für einen nicht zertifizierten Kanal (B) eine zweite Kennung (F) ermittelt wird, wobei das elektronische Gerät (EG) seinen Betrieb nur dann aufnimmt, wenn bei der Abfrage der Kennung der einzelnen Kanäle (A, B) zumindest einmal die erste Kennung (T) auftritt.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß die Abfrage der Kennung der einzelnen Kanäle (A, B) sequentiell erfolgt.

8. Verfahren nach Anspruch 6 oder 7, dadurch gekennzeichnet, daß die Kennung des nicht zertifizierten Kanals (B) nach einer vorggebbaren, von erkannten Fehlern freien Zeitspanne von der zweiten Kennung (F) auf die erste Kennung (T) gewechselt wird.

EG